Bent and $\mathbb{Z}_{2^k}$-bent functions from spread-like partitions

Wilfried Meidl[*] and Isabel Pirsic[*]

[*]RICAM, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

Abstract

Bent functions from a vector space $\mathbb{V}_n$ over $\mathbb{F}_2$ of even dimension $n = 2m$ into the cyclic group $\mathbb{Z}_{2^k}$, or equivalently, relative difference sets in $\mathbb{V}_n \times \mathbb{Z}_{2^k}$ with forbidden subgroup $\mathbb{Z}_{2^k}$, can be obtained from spreads of $\mathbb{V}_n$ for any $k \le n/2$. In this talk we show the existence of bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$, $k \ge 3$, which do not come from the spread construction. We present a construction of bent functions from $\mathbb{V}_n$ into $\mathbb{Z}_{2^k}$, $k \le n/6$, (and more general, into any abelian group of order 2^k) obtained from partitions of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, which can be seen as a generalization of the Desarguesian spread. As for the spreads, the union of a certain fixed number of sets of these partitions is always the support of a Boolean bent function. Finally we discuss generalizations to odd characteristic.

1 Introduction

Let $(A, +_A)$, $(B, +_B)$ be finite abelian groups. A function f from A to B is called a *bent function* if

$$|\sum_{x\in A} \chi(x, f(x))| = \sqrt{|A|} \qquad (1)$$

for every character χ of $A \times B$ which is nontrivial on B. Equivalently, $f : A \to B$ is bent if the graph of f, $G = \{(x, f(x)) : x \in A\}$, is a *relative difference set* in $A \times B$ relative to B.

In the classical case, $A = \mathbb{V}_n$ and $B = \mathbb{V}_m$ are elementary abelian 2-groups, i.e., they are vector spaces of dimension n and m respectively over the prime field $\mathbb{F}_2$. By (1), $F : \mathbb{V}_n \to \mathbb{V}_m$ is bent, if $m > 1$ also called *vectorial bent*, if and only if the character sum

$$\mathcal{W}_f(a, b) = \sum_{x\in\mathbb{V}_n} (-1)^{\langle a,f(x)\rangle_m \oplus + \langle b,x\rangle_n}$$

has absolute value $2^{n/2}$ for all nonzero $a \in \mathbb{V}_m$ and $b \in \mathbb{V}_n$, (here $\langle , \rangle_k$ denotes an inner product in $\mathbb{V}_k$). As is well known, n must then be even and m can be at most $n/2$. There are many examples and constructions of Boolean bent functions ($m = 1$) in the literature. Even several classes of bent functions from $\mathbb{V}_n$ to $\mathbb{V}_{n/2}$ are known, such as Maiorana-McFarland functions, Dillons H-class, see [2], and Kasami bent functions, cf.[1]. A particularly interesting construction is the (partial) spread construction, as it works not only for functions from $\mathbb{V}_n$ to elementary abelian groups $\mathbb{V}_k$, but for functions from $\mathbb{V}_n$ to any abelian group B of order 2^k, $k \le m = n/2$.

Recall that a *partial spread* $\mathcal{S}$ of $\mathbb{V}_n$, $n = 2m$, is a set of m-dimensional subspaces of $\mathbb{V}_n$ which pairwise intersect trivially. If $|\mathcal{S}| = 2^m + 1$, hence every nonzero element of $\mathbb{V}_n$ is in exactly one of those subspaces, then $\mathcal{S}$ is called a *(complete) spread*. The standard example is the Desarguesian spread, which has for $\mathbb{V}_n = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ the representation $\mathcal{S} = \{U, U_s : s \in \mathbb{F}_{2^m}\}$, with $U = \{(0, y) : y \in \mathbb{F}_{2^m}\}$ and for $s \in \mathbb{F}_{2^m}$, $U_s = \{(x, sx) : x \in \mathbb{F}_{2^m}\}$.

Given a (complete) spread $\mathcal{S}$ of $\mathbb{V}_n$, we obtain a bent function from $\mathbb{V}_n$ to B, $|B| = 2^k$, $k \le n/2$, as follows.

- For every element γ of B, except from w.l.o.g. $0 \in B$, we assign the nonzero elements of exactly 2^{m-k} elements of $\mathcal{S}$ to the preimage of γ.

- All other elements, i.e., the elements of $2^{m-k}+1$ elements of $\mathcal{S}$, are mapped to $0 \in B$.

From this general construction we also infer that the union of any $2^{m-1}+1$ elements of $\mathcal{S}$ is always the support of a Boolean bent function.

In this talk we are interested in bent functions from $\mathbb{V}_n$ to the cyclic group $\mathbb{Z}_{2^k}$, equivalently in relative difference sets in $\mathbb{V}_n \times \mathbb{Z}_{2^k}$ with forbidden subgroup $\mathbb{Z}_{2^k}$. By (1), this are functions f for which

$$\mathcal{H}_f(a,b) = \sum_{x\in\mathbb{V}_n} \zeta_{2^k}^{af(x)}(-1)^{\langle b,x\rangle},$$

where ζ_{2^k} is a complex primitive 2^kth root of unity, has absolute value $2^{n/2}$ for all nonzero $a \in \mathbb{Z}_{2^k}$ and $b \in \mathbb{V}_n$. Again such functions can only exist for $m \le n/2$, [10]. We remark that functions $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ satisfying the much weaker condition that $|\mathcal{H}_f(1,b)| = 2^{n/2}$ for all $b \in \mathbb{V}_n$ are referred to as *generalized bent functions*. They have been intensively studied in many papers, see [3, 4, 5, 6, 7, 8, 11]. If not also bent, generalized bent functions do not correspond to relative difference sets.

Bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$ can certainly be obtained with the spread construction. As far as we are aware, for $k \ge 3$ no construction is known that does not come from spread or a partial spread. In this talk we ask the question whether, and for which $k \ge 3$, there exist such bent functions that do not come from (partial) spreads. We present a construction of bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$, $k \le n/6$. With an argument via the algebraic degree of associated Boolean bent functions we show that this construction does not come from (partial) spreads. From the construction we infer partitions of $\mathbb{V}_n$ that have similar properties as spreads, in fact can be interpreted as a generalization of the Desarguesian spread. In particular, the union of a certain fixed number of sets of these partitions is always the support of a Boolean bent function.

2 Results

As we have to distinguish addition in different structures, we denote the addition in the complex numbers and in the ring $\mathbb{Z}_{2^k}$ by $+$, the addition in the elementary abelian groups $\mathbb{F}_2$, $\mathbb{V}_n$ and $\mathbb{F}_{2^m}$ is denoted by $\oplus$.

Let f be a function from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$, then we can write f as

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x)$$

for uniquely determined Boolean functions a_j, $0 \le j \le k-1$, from $\mathbb{V}_n$ to $\mathbb{F}_2$.

As ingredients for our construction we will use the following facts.

- A function $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ is bent if and only if $2^t f$ is generalized bent for all t, $0 \le t \le k-1$.
- $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x)$ is generalized bent if and only if all Boolean functions in the affine space of Boolean functions $\mathcal{A} = a_{k-1} \oplus \langle a_{k-2}, \ldots, a_0\rangle$ are bent, and for any three functions $b_0, b_1, b_2 \in \mathcal{A}$ we have

  $$(b_0 \oplus b_1 \oplus b_2)^* = b_0^* \oplus b_1^* \oplus b_2^*,$$

  where b^* denotes the dual of a Boolean bent function b, see [3].
- Let d, e be integers such that $\gcd(2^m-1, d) = 1$ and $ed \equiv 1 \bmod 2^m-1$, and suppose that $\beta_0, \beta_1, \beta_2$ satisfy

  $$(\beta_0 \oplus \beta_1 \oplus \beta_2)^{-e} = \beta_0^{-e} \oplus \beta_1^{-e} \oplus \beta_2^{-e}.$$

  Then the Boolean bent functions $b_i(x) = \mathrm{Tr}_m(\beta_i x y^d)$, $i = 0, 1, 2$, satisfy $(b_0 \oplus b_1 \oplus b_2)^* = b_0^* \oplus b_1^* \oplus b_2^*$, see [9].

We will then show the following Theorem.

Theorem 2.1 *Let m, j be integers such that* $\gcd(2^m-1, 2^j+1) = 1$ *and* $\gcd(2^m-1, 2^j-1) = 2^k-1$*, let $e = 2^m - 2^j - 2$, and let d be the inverse of e modulo $2^m - 1$. Then for a basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\}$ of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$, the functions f_1 and f_2 given as*

$$f_1(x) = \sum_{i=0}^{k-1} \mathrm{Tr}_m(\alpha_i x y^d) 2^i, \qquad f_2(x) = \sum_{i=0}^{k-1} \mathrm{Tr}_m(\alpha_i^{-e} x^e y) 2^i \tag{2}$$

are bent functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$.

With an argument via algebraic degrees, we will then conclude

Corollary 2.2 *Let m and $j > 0$ be integers such that* $\gcd(2^m-1, 2^j+1) = 1$ *and* $\gcd(2^m-1, 2^j-1) = 2^k-1$*, and let e, d, α_i, $0 \le i \le k-1$, be as in Theorem 2.1. Then the functions f_1, f_2 in* (2) *are bent functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$, which do not come from partial spreads.*

The final part of the talk is dedicated to partitions which we infer from the functions in Theorem 2.1

Let m, k be integers such that k divides m and $\gcd(2^m-1, 2^k+1) = 1$, let $e = 2^m - 2^k - 2$ and d such that $de \equiv 1 \bmod 2^m - 1$. For an element $s \in \mathbb{F}_{2^m}$ define

$$U_s := \{(x, sx^{-e}) \ : \ x \in \mathbb{F}_{2^m}\},\ U_s^* = U_s \setminus \{(0,0)\},\ \text{and}\ U = \{(0, y) \ : \ y \in \mathbb{F}_{2^m}\}.$$

Then U, U_s^*, $s \in \mathbb{F}_{2^m}$, form a partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Note that U, U_s, $s \in \mathbb{F}_{2^m}$, are the subspaces of the Desarguesian spread if $2^k + 1 \equiv -e \equiv 1 \bmod 2^m - 1$ (more general, if $-e \equiv 2^v \bmod 2^m - 1$). Also note that U_s is not a subspace if we do not have $-e \equiv 2^v \bmod 2^m - 1$ for some integer v.

Similarly, for an element $s \in \mathbb{F}_{2^m}$ we define

$$V_s := \{(x^{-d}s, x) \ : \ x \in \mathbb{F}_{2^m}\},\ V_s^* = V_s \setminus \{(0,0)\},\ \text{and}\ V = \{(x, 0) \ : \ x \in \mathbb{F}_{2^m}\}.$$

Note that as above for the sets U and U_s, if $-d \equiv 2^v \bmod 2^m - 1$, then V_s and V are the subspaces of the Desarguesian spread.

For the divisor k of m and an element γ of $\mathbb{F}_{2^k}$ let

$$\mathcal{A}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{2^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} U_s^* \quad \text{and} \quad \mathcal{B}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{2^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} V_s^*.$$

With this definitions we obtain two partitions of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$

$$\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{2^m}\}$$
$$\Gamma_2 = \{V, \mathcal{B}(\gamma); \gamma \in \mathbb{F}_{2^m}\},$$

that have similar properties as spreads have:

Theorem 2.3 *Let m, k be integers such that k divides m and* $\gcd(2^m-1, 2^k+1) = 1$*, and let $\pi(i) = \gamma_i$ be a one-to-one map from $\mathbb{Z}_{2^k}$ to $\mathbb{F}_{2^k}$. Define functions $f_A, f_B : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{Z}_{2^k}$ as follows:*

- *If $(x, y) \in \mathcal{A}(\gamma_i)$ then $f_A(x, y) = i$, and, w.l.o.g., $f_A(0, y) = 0$ for all $y \in \mathbb{F}_{2^m}$;*
- *If $(x, y) \in \mathcal{B}(\gamma_i)$ then $f_B(x, y) = i$, and, w.l.o.g., $f(x, 0) = 0$ for all $x \in \mathbb{F}_{2^m}$.*

Then f_A, f_B are bent functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$.

Theorem 2.4 *Let m, k be integers such that k divides m and* $\gcd(2^m-1, 2^k+1) = 1$*, let $e = 2^m - 2^k - 2$ and d such that $de \equiv 1 \bmod 2^m - 1$.*

I. Every Boolean function of which the support is the union of 2^{k-1} of the sets $\mathcal{A}(\gamma)$ is a bent function. Likewise, their complements, i.e., the Boolean functions with U and 2^{k-1} of the sets $\mathcal{A}(\gamma)$ as their support, are bent.

II. Every Boolean function of which the support is the union of 2^{k-1} of the sets $\mathcal{B}(\gamma)$ is a bent function. Likewise the Boolean functions with V and 2^{k-1} of the sets $\mathcal{B}(\gamma)$ as their support, are bent.

The duals of the bent functions of the class in I are in the class in II (and vice versa).

Remark 2.5 *(i) In the special case $k = m$, the partitions Γ_1, Γ_2 reduce to a Desarguesian spread partition, and f in Theorem 2.3 is a spread function on the complete Desarguesian spread. Theorem 2.4 describes then the well known PS^-_{ap} and PS^+_{ap} bent functions, cf. [2]. Hence we may see the bent functions in Theorem 2.3, and the Boolean bent functions in Theorem 2.4 as generalizations of the Desarguesian spread bent functions.*

(ii) As for the classical spread functions, also the proof of Theorem 2.3, holds not only for functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$, but for functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to any abelian group B of order 2^k. The bentness is a property of the partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. For instance, also many more vectorial bent functions in dimension k are obtained.

(iii) Clearly, as for the spreads, the partitions Γ_1 and Γ_2 represent a whole equivalence class of partitions. Numerically we confirmed that in general Γ_1 and Γ_2 are not equivalent.

References

[1] C. Carlet, Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Des. Codes Cryptogr. 59 (2011), 89–109.

[2] J.F. Dillon, Elementary Hadamard difference sets, Ph.D. dissertation, University of Maryland, 1974.

[3] S. Hodžić, W. Meidl, E. Pasalic, Full characterization of generalized bent functions as (semi)-bent spaces, their dual, and the Gray image. IEEE Trans. Inform. Theory 64 (2018), 5432–5440.

[4] T. Martinsen, W. Meidl, P. Stanica, Generalized bent functions and their gray images. In: Arithmetic of finite fields, Lecture Notes in Comput. Sci., 10064, pp. 160–173, Springer, Cham, 2016.

[5] T. Martinsen, W. Meidl, P. Stanica, Partial spread and vectorial generalized bent functions. Des. Codes Cryptogr. 85 (2017), 1–13.

[6] W. Meidl, A secondary construction of bent functions, octal gbent functions and their duals. Math. Comput. Simulation 143 (2018), 57–64.

[7] W. Meidl, A. Pott, Generalized bent functions into $\mathbb{Z}_{p^k}$ from the partial spread and the Maiorana-McFarland class, Cryptogr. Commun. 11 (2019), 1233–1245.

[8] S. Mesnager, C. Tang, Y. Qi, L. Wang, B. Wu, K. Feng, Further results on generalized bent functions and their complete characterization. IEEE Trans. Inform. Theory 64 (2018), 5441–5452.

[9] S. Mesnager, Several new infinite families of bent functions and their duals. IEEE Trans. Inform. Theory 60 (2014), no. 7, 4397–4407.

[10] K. Nyberg, Perfect nonlinear S-boxes, In: Advances in cryptology–EUROCRYPT '91 (Brighton, 1991), Lecture Notes in Comput. Sci., 547, pp. 378–386, Springer, Berlin, 1991.

[11] C. Tang, C. Xiang, Y. Qi, K. Feng, Complete characterization of generalized bent and 2^k-bent Boolean functions. IEEE Trans. Inform. Theory 63 (2017), 4668–4674.